REMARKS/ARGUMENTS

The rejection of claims 1-4, 11-15, 19, 22, 28, 30-32 and 34-36 under 35 USC §103 as allegedly being made "obvious" based on Hile '776 in view of newly cited Sorkin '017 is respectfully traversed.

Applicant's claim 1 is directed to a server that is situated between (a) a plurality of inside terminals and (b) other outside terminals such that incoming/outgoing emails to/from the inside terminals (with respect to the outside terminals) must pass through the server.

The intervening server generates or receives log data relating to one or more traffic characteristics associated with such email. This traffic log data is analyzed in accordance with a predetermined criterion so as to identify email that satisfy that criterion. The destination of thus identified email is identified and a message is sent to each of the thus identified destinations to request suspension of delivery of such identified email.

Hile is first of all deficient for a reason now recognized by the Examiner. Namely, Hile has nothing whatever to do with log data of any kind—let alone traffic log data. Indeed, to the contrary, Hile attempts to detect computer viruses by tediously analyzing each and every character of incoming data streams—so as to hopefully detect any one of multiple search strings representing the signatures of known computer viruses. Such prior art approaches have significant downsides—and are antithetical to the quite different approach (of analyzing traffic log data) required by applicant's claim 1.

Furthermore, even if Hile succeeds in finding what is believed to be a known computer virus in the content of some email, the Hile system does not react by (a)

identifying the destination of a so-identified email and (b) sending a message to each such identified destination requesting suspension of delivery of the identified electronic messages. Indeed, Hile teaches one to prevent the detected virus from remaining on a "destination" storage medium (i.e., instead of merely requesting suspension of delivery of such identified email, Hile has already delivered at least part of the message but takes steps to prevent such from remaining at the destination).

The Examiner's style of comment appears to be to quote or paraphrase passages from applicant's claims and then intersperse bolded comments/assertions.

For example, it appears the Examiner believes that the Hile "Abstract" teaches the testing of log data when it is in transit between a source and destination. The Examiner also appears to assert that the Hile Abstract teaches performance of such testing as a function of "the traffic characteristic" of incoming data.

However, the Hile abstract does not mention a single type of "log data" – nor does it in any way suggest testing "log data" as a function of any sort of "traffic characteristic" associated with incoming data. The entirety of the Hile Abstract is quoted below for the Examiner's convenience:

> Data is tested in transit between a source medium and a destination medium, such as between two computer communicating over a telecommunications link or network. Each character of the incoming data stream is tested using a finite state machine which is capable of testing against multiple search strings representing the signatures of multiple known computer viruses. When a virus is detected the incoming data is prevented from remaining on the destination storage medium. Both hardware and software implementations are envisioned.

In particular, Hile does not teach the features alleged to be present by the Examiner. Furthermore, the Hile Abstract actually teaches directly away from testing of log data

because the Abstract makes clear that is not log data (of any kind) that is to be tested but, instead, each character of an incoming data stream.

Claim 1 also requires an analyzing means to analyze log data in accordance with a predetermined criterion thus to identify electronic messages that satisfy such criterion. Here, the Examiner asserts such a teaching to be found in Hile at column 4 lines 11-13:

> When the incoming data stream has been error checked and the input buffer becomes filled, in a conventional data communications system, the data in buffer 30 would be stored on the destination medium 24b. The present invention intervenes at this point by subjecting the buffered data to a character by character virus signature string search analysis depicted at 32....[4:7-13]

Once again, there is no teaching at all here for analyzing log data of any kind. Instead, the teaching of Hile is directly to the contrary in that the explicit direction is to subject the buffered data to a character by character virus signature string search analysis.

Claim 1 also requires an identifying means to identify the destination of the identified electronic messages and processing means arranged to send a message to each of the identified destinations requesting suspension of delivery of the identified electronic messages. Here, the Examiner relies upon column 2, lines 21-25 for the proposition that Hile involves sending of messages to a computer system having a "destination storage medium" and relies upon column 3, lines 7-10 and/or the Hile "Abstract" for the sending of a message to each identified destination requesting suspension of delivery of the identified electronic message.

However, the Examiner's own paraphrasing of an extract from the Hile Abstract reveals that the Hile system does not send a message to each identified destination requesting suspension of delivery but instead, actively prevents detecting incoming infected data from remaining on the destination storage medium.

Indeed, the closest analogy to applicant's sending of a message to each identified destination appears to be the Hile sending of an alert "warning message" to be displayed on the computer system monitor. However, in the context of Hile, this is presumably the monitoring computer system monitor (e.g., see the "alert user" box 36 in Figures 1 and 2 that appears to be associated with the intermediate search engine).

Given such repeated fundamental deficiencies of Hile with respect to numerous aspects of claim 1, it is puzzling that the Examiner only appears to recognize a single difference: "Hile differs from the claimed invention is [*sic*: in] that log data is not taught in Hile."

To supply at least this single admitted deficiency of Hile, the Examiner now relies upon Sorkin '017. However, while Sorkin does have some relevance to a "log" file, it does not appear to have teaching or suggestion of a traffic log file—nor much else that is relevant to applicant's invention. Indeed, as will be explained in more detail below, both Hile and Sorkin teachings may be used in parallel and concurrently—and still not teach or suggest the applicant's invention as claimed even in independent claim 1.

As just noted, in the Hile system a virus within a file is detected by scanning or testing the file content itself for known virus signatures. The present invention provides an advantage over Hile, in that it is not required, when examining log data relating to traffic characteristics, to scan for virus signatures. This advantage is particularly useful when the virus signatures are not known.

Of course if virus signatures are known, the need to examine traffic log data is reduced, since known viruses can be detected through their known signatures. Thus the use of log data relating to traffic represents a possible alternative to the use of virus

signatures. A person of ordinary skill faced with the teachings of Hile would therefore not seek to examine or generate log data relating to traffic characteristics. By providing an alternative that in no way relies upon use of log data of any kind, Hile teaches away from the present invention.

The Sorkin log file data brings a skilled person no closer to the applicant's claimed invention. Sorkin is concerned with detecting a hacker intrusion, and the analyzed log files are a log of the intruder's actions—including commands and/or keystrokes, as well as information on processes running within the machine subject to attack by the hacker (e.g., see paragraph [0177].

Clearly, details of a given hacker's actions (and running processes) are different from traffic characteristics as claimed. Whereas "traffic" implies data traveling between machines, details of hacker actions and processes running in a "cage" as disclosed in Sorkin relate to details of operation of the specific machine being hacked; that is, the operation of a single machine.

Not only is the Sorkin log data a very different type of log data than applicant has claimed, the Sorkin analysis is performed for a very different reason. A skilled person would see that whereas in Hile the data is analyzed to search for a virus, in Sorkin hacker processes and commands are analyzed to detect an intruder through their own actions.

It is not particularly helpful to look for evidence of hacker actions when scanning emails for viruses as is done in Hile, since the type of data representative of a virus signature is likely to be very different from the type of hacker action log data indicative that a hacker is accessing a system.

In fact, it is evident that were the type of log file analysis performed in Sorkin to be performed on e-mails or other transmitted data as is done in Hile, then viruses would not be detected. Conversely, were the system of Sorkin to be modified such that a machine is scanned for viruses with a view to detecting a hacker attack, evidence of an incoming virus would not necessarily indicate a hacker attack on the machine, but rather that (as is commonly the case) malicious software had previously been inadvertently downloaded by a legitimate user. For these reasons, a person of ordinary skill would not seek to combine the teachings of Sorkin and Hile—unless one wanted to simultaneously address two quite different problems.

In that case, a skilled person would see that the system of Hile and Sorkin are complementary, and would seek to implement both rather than substituting parts of one system with part of the other system. That is, a skilled person would use the system of Sorkin to attempt to prevent intruder attack, and, if such an attach were nevertheless successful, would then use the system of Hile to detect the consequences, if any, of the attack.

In any event, even a complete combination of Hile and Sorkin cannot lead to the presently claimed invention, since neither discloses analysis of data relating to traffic characteristics. Clearly, the hacker action log data as disclosed in Sorkin is very different to traffic log data relating to traffic characteristics—and nothing in Sorkin teaches or even suggests how to analyze traffic log data in a way that is compatible with the teachings of Hile. Furthermore, the "log" data in Sorkin is analyzed for different reasons than those in the applicant's invention (i.e., Sorkin determines hacker attack

rather than applicant's detecting of suspicious traffic patterns), thereby teaching away from the present invention.

Independent method claim 12 also requires method steps parallel to the features already discussed above with respect to independent claim 1. Accordingly, independent claim 12 is also patentably distinct from any possible teaching or suggestion of either or both of the cited references.

Independent claim 31 requires a computer program configured to perform steps which, when executed, invite a user to input at the user interface send instructions for sending one or more electronic messages: to determine if traffic log data meets a predetermined criterion relating to the electronic messages; if that criterion is met, to invite the user to input at the user interface a confirmation input to confirm the send instructions; upon receipt of the confirmation input, to actually go ahead and transmit the electronic messages from the terminal and, finally, to transmit authentication data associable with the transmitted electronic messages.

With respect to claim 31, the Examiner appears to rely entirely only upon Hile. Once again, as already noted above, the Hile Abstract does not have anything to do with testing log data—of any kind, let alone traffic log data.

Furthermore, contrary to the Examiner's assertions, Hile at column 7, line 3 does not have anything to do with inviting a user to input a confirmation input to confirm send instructions. Instead, this passage of Hile appears to have reference only to the processing of received messages. Furthermore, a "virus detected flag" has nothing to do with traffic log data. Similarly, the last two integers of claim 31 have to do with transmitting outgoing messages—while the passages referred to by the Examiner have

to do with the processing of incoming received messages (and with respect to a completely different kind of processing).

The Examiner's reference to the fact that Hile gives examples written in the C programming language does not appear to have relevance to the applicant's claimed invention.

Applicant's independent claim 32 requires a computer program which, when running on a computer, also invites the user to input send instructions for sending one or more specified electronic messages wherein the computer program is also configured, when executed, to invite input of a confirmation of the send instructions and to later only permit the user to send the electronic message once the user has input a confirmation instruction, etc. Here, the Examiner also appears to rely only upon Hile and makes only comments already discussed above with respect to independent claim 31.

Applicant's independent claim 36 is directed to a server which includes a receiving means for generating or receiving traffic log data relating to email, analyzing means to analyze the traffic log data in accordance with specified criteria, identifying means for identifying the destination of the identified email and a processor arranged to send a message to each identified destination requesting suspension of delivery of the thus identified electronic messages.

Here, the Examiner also appears to rely entirely upon Hile. As previously noted, Hile does not have any means for generating or receiving traffic log data. Nor does Hile have any analyzing means for analyzing traffic log data. The Examiner's various references to column 1, lines 32-35; and column 3, lines 7-10 and 45-48 are entirely off

the point—for reasons such as those already noted above. For example, the Examiner relies upon 1:32-35 for an analyzing means to analyze traffic log data in accordance with a specified criterion, etc. However, this passage at column 1 simply refers to prior art virus scanning programs which "read the file stored on a storage medium, looking for known virus signatures". As already noted above, this is the antithesis of applicant's claimed invention where it is traffic log data that is analyzed—not the entire file content.

As for the claim 36 requirement of a processing means for sending a message to each of the identified destinations requesting suspension of delivery of the identified email, the Examiner merely relies upon 3:7-10 – but this has nothing whatever to do with requesting suspension of delivery at each identified destination, etc. Instead, this passage merely explains that the Hile invention will be described in conjunction with a communications system which can be used to send and receive data via modems over a telecommunications link. Of course, that is true—but it is entirely beside the point with respect to applicant's claimed invention in claim 36.

Given such fundamental and far reaching deficiencies of both Hile and Sorkin with respect to the above-discussed features of the rejected independent claims, it is not believed necessary at this time to discuss the additional deficiencies of this allegedly "obvious" combination of references with respect to other features of the rejected independent claims or with respect to the additional features of the rejected dependent claims.

The rejection of claims 5-7, 8-10, 16-18, 20, 21, 25-29 and 33 under 35 USC §103 as allegedly being made "obvious" based on Hile '776 in view of Kim '440 is also respectfully traversed.

Exemplary deficiencies of Hile '776 have already been noted above with respect to parent claims of dependent claims 5-7, 8-10, 16-18, 25-29 and 33. Kim does not supply even those deficiencies. Accordingly, it is not believed necessary at this time to discuss the additional deficiencies of this allegedly "obvious" combination of references with respect to these dependent claims.

Independent method claim 20 is directed towards a method of identifying email activity within an organization having a plurality of users, each of which is connected with an organizational unit. Claim 20 requires receiving traffic log data defining at least one message traffic characteristic emanating from a user and relating to email sent by a user; analyzing the received traffic data in accordance with a specified criterion so as to identify certain email satisfying that criteria; receiving data identifying a mapping between users and the organizational units to which those users belong; displaying a plurality of images, each representative of an organizational unit; outputting data identifying the users who originated the email to satisfy the criterion; identifying, from the mapping, which of the organizational units the users belong to; and inserting, on an image corresponding to the identified organizational unit, visual identifiers representative of the volume or type of identified email.

Here, the Examiner first appears to rely entirely upon the single reference to Hile—although the organization of the Office Action at pages 15-16 is a little confusing as to whether the secondary reference to Kim is supposed to be used with respect to claim 20 as well as claim 21.

In any event, the Examiner's allegations concerning Hile—and Kim—are respectfully traversed.

Contrary to the Examiner's allegation, Hile at column 3, lines 7-10 does not teach anything about traffic log data at all. Similarly, the Hile passage at column 3, lines 45-48 has no teaching whatsoever with respect to identifying email activity within an organization having a plurality of users. Instead, this passage merely states that in a telecommunications system, the user of a second computer system often has no direct control over the integrity of files stored on the source medium—which file may be corrupted by a virus. If anything, this passage of Hile appears to be talking about a computer on one side of a virus scanning system and another computer on the other side of the virus scanning system. There is no mention of either side of the process necessarily having an organization with a plurality of users, etc.

Similarly, contrary to the Examiner's assertions, column 1, lines 32-35 of Hile does not teach analysis of received traffic log data in accordance with a specified criteria so as to identify email satisfying that criteria. Instead, Hile here teaches directly to the contrary—namely, that in other "prior art" systems (just like the Hile system), it is the entire file that must be scanned for known virus signatures.

As noted earlier, after an intervening section regarding claim 21, the Examiner does at page 16 of the Office Action admit that Hile differs from the claimed invention with respect to displaying certain types of data. Even here, the Examiner appears to effectively ignore the claim 20 requirement for receiving data identifying a mapping between users and organizational units—together with displaying a plurality of images, each representative of an organizational unit.

In any event, in an effort to supply the admitted deficiencies of Hile, the Examiner relies upon Kim '440. In particular, the Examiner relies upon the Abstract of Kim and

the passage at column 11, lines 48-52. However, these portions of Kim merely describe a computer system 500 that happens to include a generic display or monitor 502, screen 504, cabinet 506, keyboard 508 and mouse 510. While there obviously would be some sort of graphical user interface (GUI) involved, Kim totally fails to teach anything about receiving data identifying a mapping between users and the organizational units to which the users belong, displaying a plurality of images, each representative of an organizational unit, etc., as explicitly required in claim 20. Indeed, the Examiner's comments concerning Hile and/or Kim simply avoid even referencing these passages from applicant's claim 20.

Neither is there anything in either of the cited references about identifying, from the mapping, which of the organizational units the users belong to and then inserting on an image corresponding to the identified organizational units, visual identifiers representative of the volume or type of identified email.

Given such fundamental deficiencies of Hile and/or Kim with respect to independent claim 20, it is not believed necessary to discuss further deficiencies of this allegedly "obvious" combination of references with respect to other features of claim 20 and/or rejected dependent claim 21.

The Examiner's separate restatement of the rejection of claims 25-29 and 33 under 35 USC §103 as allegedly being "obvious" based on Hile in view of Kim (e.g., see pages 19-20) is also respectfully traversed for reasons already noted above with respect to the apparent identical rejection.

The rejection of claims 23 and 24 under 35 USC §103 as allegedly being made "obvious" based on Hile in further view of Miloslavsky '787 is also respectfully traversed.

Independent claim 23 is directed to a server configured to send outgoing email on behalf of terminals connected thereto and to deliver incoming email to those terminals, each terminal being accessed by one or more users. Claim 23 requires the server to include logging means to generate traffic log data relating to one or more traffic characteristics associated with the email. Claim 23 further requires the server to include analyzing means to analyze the received traffic log data in accordance with a specified criterion so as to identify those electronic messages that satisfy that criterion.

The Examiner's discussion of Hile is deficient for reasons already noted above. Namely, Hile does not have a single thing to do with traffic data—let alone traffic log data relating to one or more traffic characteristics associated with email. To the contrary, Hile is directed towards analyzing each and every character in the content of every received file looking for character strings constituting a virus "signature". There is no attempt whatsoever anywhere in Hile to analyze traffic data of any kind. The Examiner's reliance upon Hile at column 1, lines 32-35 is deficient for reasons already noted. First of all, it deals with a prior art IBM virus scanning program. Secondly, the prior art system being described apparently is relatively similar to the Hile system in that the entire file content is scanned looking for a virus "signature". There is nothing at column 1, lines 32-35 having to do with analyzing any traffic log data—let alone with respect to a predetermined criterion.

As earlier, the Examiner asserts that the only relevant difference between Hile and the claimed invention is a failure to generate or receive log data relating to one or more traffic characteristics associated with email. When properly understood, it will be recognized by those skilled in the art that Hile is teaching an entirely different

technique—one for detecting virus signatures—having nothing to do with analyzing log file data of any kind but, instead, requiring one to analyze the entire content of each file, character by character.

Miloslavsky merely teaches a system for routing email. In order to know which persons are present at work and available to receive and answer a given email, at the time it is received, a real-time record is maintained of employees that are present and at work—i.e., so that incoming emails can be properly directed for appropriate responses as soon as possible, etc. The Examiner refers to this record as a "log" and cites to "column 7, lines 50-54" for support. Actually, there are no lines 50-54 at column 7—and the undersigned cannot find the use of the word "log" elsewhere on any other column at these or any other lines. However, even if it is assumed *arguendo* that such statistics might be considered a "log" of those people who are presently present and available to take incoming email traffic, that is clearly not a traffic log. That is, statistics identifying employees that are present and available for work duties is not a traffic log data relating to one or more traffic characteristics associated with electronic messages. Nor does it have any means for analyzing received traffic log data in accordance with a specified criterion so as to identify email that satisfy that particular criterion (i.e., as a function of email traffic log data).

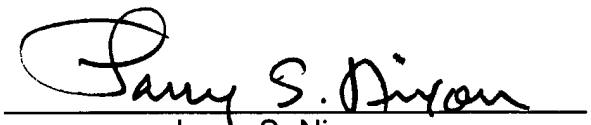
Dependent claim 24 further requires the identifying means to identify the destination of the identified email and processing means to send a message to each such identified destination requesting suspension of delivery of the identified email. Here, the Examiner does not even cite to Miloslavsky but, instead, cites back to the irrelevant Hile at Figure 1, step 40 and/or the Abstract and/or column 3, lines 7-10. As

already noted, none of this cited Hile teaching teaches or suggests sending a message to each identified destination requesting suspension of delivery of the identified electronic messages, etc.

Accordingly, this entire application is now believed to be in allowable condition and a formal notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

Larry S. Nixon
Reg. No. 25,640

LSN:ejs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100